This record is a partial extract of the original cable. The full text of the original cable is not available.

260952Z Oct 05

UNCLAS SECTION 01 OF 05 PARIS 007314

SIPDIS

SENSITIVE

PASS SEC FOR SBOONE
PASS FEDERAL RESERVE
STATE FOR EB/IFD AND EUR/WE
TREASURY FOR DO/IM MSOBEL AND LHULL
TREASURY ALSO FOR DO/IMB AND DO/E WDINKELACKER
LABOR FOR ILAB
USDOC FOR 4212/MAC/EUR/OEUR

E.O. 12958: N/A
TAGS: EFIN ECON FR
SUBJECT: GOF PROGRESS ON SARBANES OXLEY WHISTLEBLOWER DRAFT GUIDELINES

SENSITIVE BUT UNCLASSIFIED. NOT FOR INTERNET DISTRIBUTION

¶1. (SBU) SUMMARY AND ACTION REQUEST: We have received draft French guidelines that would permit companies to use anonymous hotlines per Sarbanes Oxley requirements, and would welcome Washington views on the draft, ideally before November 8. END SUMMARY.

¶2. (SBU) Staff members from the French privacy protection agency, CNIL, which blocked firms from implementing whistleblower hotlines in France, have issued draft guidelines that would allow hotlines under certain conditions. CNIL has circulated the draft informally to interested parties, to get input before presenting the draft to its Board of Commissioners for final approval. The next Board meeting is expected to occur on November 8.

¶3. (SBU) Separately, we met with Marc Guillaume, Director of Civil Affairs in the Ministry of Justice (upon which the CNIL depends). His view is that Sarbanes Oxley requirements are illegal under international law, inasmuch as they have extraterritorial effects that are not based on the concepts of personal or territorial jurisdiction. He suggested the best solution would be to amend the US law, citing a number of other laws that had been deemed extraterritorial and subsequently had been amended.

¶4. (SBU) We have also met with a number of interested parties to discuss at length the draft text. Most are encouraged by the possibility that hotlines will be permitted. Some remain concerned that the French guidelines still are too narrow to accommodate reporting obligations that arise outside of the accounting and auditing areas covered by Sarbanes Oxley. Others expressed concern about a German decision that struck down a hotline set up by Wal-Mart, because it had failed to have its code of conduct approved by the German Works Council prior to implementation.

¶5. (SBU) The draft text, in its English translation, reads as follows:

BEGIN TEXT:
Draft guidelines for the implementation of whistleblowing schemes under the French Data Protection Act of January 6th, 1978, as amended on August 6th, 2004

Warning : This document was prepared by the CNIL's internal departments, under the supervision of Mr. Hubert Bouchet, commissioner in charge of the sector of labor affairs. It has not been submitted to, and is not binding on, the Commission (CNIL). It will be submitted to the Commission for approval after official consultation of public authorities, professional organizations, trade unions and expert associations.

The Commission nationale de l'informatique et des libertes (CNIL) has noted the recent development in France of procedures enabling employees to report their colleagues' allegedly law- or corporate policy-breaching behaviors in the office ("whistleblowing schemes").

Such schemes are neither allowed nor banned under current Labor Code provisions. They rely on the processing of personal data and therefore, are subjected to the provisions of the January 6, 1978 Act, whether the processing is computer- or paper-based.

The CNIL in May 2005 refused to authorize two specific whistleblowing schemes . However, it has no objection in principle to such schemes, provided the rights of individuals directly or indirectly incriminated through them are guaranteed with regard to personal data protection rules. Indeed, such individuals, in addition to the rights which they are granted under labor law if disciplinary actions are initiated against them, are entitled to specific rights under the Data Protection

Act or under European directive 95/46/CE of October 24, 1995 when data relating to them are processed : right to such data being collected fairly; right to be informed that such data is being processed; right to object to such processing for legitimate reasons, right to have any inaccurate, incomplete, ambiguous or outdated information rectified or removed.

The CNIL has established the following guidelines in order to contribute to the implementation of whistleblowing schemes that comply with the principles set forth by the law and the directive.

1) Impact of whistleblowing schemes : subsidiary nature, limited scope, non-mandatory use

Obviously any normally operated organization requires that an alert concerning any professional problem should reach management through the natural channel of the line of command or by open reporting methods involving personnel representatives or account auditors, the latter enjoying appropriate protection and independence under French law, for that matter. However, the implementation of a whistleblowing scheme may be justified under the assumption that these information channels may not work in some circumstances.

Due to its inherently subsidiary nature, the scope of such a whistleblowing scheme should be limited. Schemes with a general and indiscriminate scope (such as those intended to ensure compliance with legal requirements, corporate policies or internal rules on business conduct, for instance) raise an automatic difficulty with regard to the Data Protection Act due to the risk of abusive or disproportionate incrimination of the professional, or even personal integrity of the employees concerned.

However, the legitimacy of whistleblowing processes implemented for the sole purpose of meeting a French legal requirement aimed at establishing reinforced internal control procedures in specific areas is indisputable. Such a requirement clearly results, for instance, from provisions relating to the internal auditing of credit institutions and investment companies (order dated March 31, 2005 amending the Banking and Financial Policy Committee ("Comite de reglementation bancaire et financiere") regulation number 97-02 dated February 21, 1997).

It appears that, under the Data Protection Act, such legitimacy may not result from the mere existence of a foreign legal provision by virtue of which a whistleblowing scheme would be implemented. This specifically applies to the provisions of Section 301(4) of the Sarbanes Oxley Act, which provide that the employees of an issuer may raise any concern with the audit committee as to questionable accounting controls or auditing matters while being assured that their reports will be processed under conditions of confidentiality and anonymity.

On the other hand, one cannot disregard the benefits of implementing whistleblowing schemes concerning financial and accounting matters to French companies directly listed in the United States or to French subsidiaries of US companies listed in the United States, which must accordingly comply with a requirement to certify their accounts to the US national securities exchanges. Obviously, ensuring that information relating to financial embezzlement and account rigging properly reaches the Board of directors is a critical concern for any issuer.

Far from being limited to the United States, initiatives were also taken in Europe (including the European Commission recommendation of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board), which are aimed at achieving the same objective as the Sarbanes-Oxley Act, i.e. reinforcing the safety of financial markets. In this context, whistleblowing schemes which are restricted to auditing and accounting issues are acceptable.

The same applies to whistleblowing systems whose purpose is to combat bribery of foreign public officials in international business transactions (OECD convention dated December 17, 1997, ratified by Act Nr.99-424 dated May 27, 1999).

In order to prevent a whistleblowing scheme from being abused into reporting facts unrelated to such specific pre-determined areas, the data controller responsible for the scheme should clearly state that its use is strictly reserved for such areas and should refrain from following on an alert made on facts that fall outside its scope.

More generally, using a whistleblowing scheme that may be deemed as legitimately put into operation should not be made compulsory for employees. Indeed the French Department for Employment, Labor and Professional Integration ("ministere de l'emploi, du travail et de l'insertion professionnelle") has stated, in a letter sent to the CNIL, that the use of whistleblowing systems should be not a requirement, but only be encouraged. (.) Making reporting mandatory would result in passing on to employees

employers' duties in terms of ensuring compliance with corporate policy. It can be argued also that the reporting requirement would breach article L120-2 of the Labor Code as a requirement out of proportion with its objective .

2) Limited categories of individuals to be involved in a whistleblowing scheme

In accordance with the proportionality principle, the categories of personnel likely to be incriminated through a whistleblowing scheme should be determined accurately, in accordance with the purposes of the implementation of the scheme. Though it is not ruled out that any member of the personnel may be involved by an alert, it is disproportionate that a whistleblowing scheme focusing e.g. on financial and accounting matters result in the incrimination of employees with no responsibility in that area.

The categories of personnel likely to make use of a whistleblowing scheme should also be determined accurately based on their ability to avail of information about the specific area concerned by the scheme. For instance, it would probably be disproportionate to allow factory workers employed at an industrial production center to have access to a whistleblowing scheme dedicated to raising concerns as to financial embezzlement or account rigging.

3) Restrictive processing of anonymous reports

The right to file anonymous reports can only increase the risk of slanderous reports. Conversely, requesting an individual's identification prior to let him/her make a report can only help increase the responsibility of the users of the process and thus reduce such a risk. As a result whistleblowing schemes should imply that the data necessary to identify the whistleblower is collected.

Protecting the whistleblower is a requirement inherent to the whistleblowing scheme. It is not the CNIL's responsibility to appreciate the means used to ensure such protection, except for one area that results clearly from the Data Protection Act. The individual's identity should be processed in a confidential manner. Specifically, it should not be disclosed to the incriminated individual based on the latter's right to access data concerning him/her specified in article 39 of the said Act.

The existence of anonymous reports, even and especially if there is no organized confidential whistleblowing system, is an unavoidable fact. It is also difficult for company officials to disregard such reports. The processing of such reports should be subject to specific precautions, particularly as to their circulation within the organization. At any rate, the organization should not encourage individuals who are likely to use the system to do so anonymously and the publicity made of such schemes inside the organization should take that point into account. This requires not to make anonymous reports easy, including by opening a dedicated telephone line that would not require the identification of the whistleblower at the beginning of the call.

4) Communication of clear and extensive information on the whistleblowing scheme

Clear and extensive information to potential users of the whistleblowing scheme should be conveyed by any appropriate means.

In accordance with article 32 of the Data Protection Act, such information should in particular include the identification of the entity in charge of the scheme, the purposes and the scope of the scheme, its optional nature, the fact that employees will not be sanctioned for not using it, the recipients of the reports, as well as the right of incriminated individuals to access and rectify their data.

Going through the line of command should be described as the normal and preferred method for handling cases where professional rules established by the law are allegedly not complied with.

Lastly, it should be clearly stated that any abuse of the system will result in disciplinary action and criminal proceedings being filed against the author of the abuse.

5) Collecting reports through dedicated means

The reports may be collected by any data processing means, whether electronic or not.

Such means should be dedicated to the whistleblowing scheme in order to prevent any diversion from its original purpose and for added data confidentiality.

6) Relevant, adequate and non-excessive data in reports

The medium on which data collected through a whistleblowing scheme is recorded should only mention objective data that is directly related to the scope of the scheme and is strictly

required for verifying the alleged facts.

The wording used to describe the nature of the reported facts should express that the facts are alleged.

7) Processing of internal reports reserved for specialists in a confidential framework

SIPDIS

The reports should be collected and processed by an entity dedicated to those issues, within the organization. There should be a limited number of individuals in charge of taking action in the report management process. These individuals should be specially trained and subjected to special, contractually-defined, confidentiality duties.

Data confidentiality should be ensured both when the data are collected and when they are disclosed or stored.

The data should not be disclosed to other legal entities unless such disclosure is required for processing the report (ex : involvement of another organization's employee, or a high-level member or management body of the respective company). In that case, the data should only be provided, in a secured manner, to the relevant body of the legal entity if it offers equivalent guarantees for the processing of such reports.

Specifically, the fact that several legal entities belong to the same group alone does not justify that a report made within a subsidiary implementing a whistleblowing scheme be necessarily disclosed to its parent company. Additionally, in the exceptional cases - mentioned in the paragraph above - where such disclosure is required to a legal entity based in a non European Union country that does not ensure an adequate level of protection in the meaning of directive 95/46/EC of October 24, 1995, the specific provisions of the Data Protection Act relating to international transfers of data should be applied (specific legal framework and information to reported individuals that the data will be transferred to such a country).

Lastly, if the organization envisages to call upon a service provider to handle the whistleblowing scheme, the latter should undertake by contract that it will not use the data for diverted purposes, that it will ensure the confidentiality thereof, meet limited data retention periods, and inform the individuals identified by the whistleblowing processing system. The company will in any case remain responsible for the processing carried out by the service provider.

8) Circulating anonymous business reports

For the purpose of evaluation of the whistleblowing scheme, the company may provide entities in charge of processing such reports within the group with any statistical information useful for the performance of their duties (such as data relating to the types of reports made and corrective action taken).

Such information should not directly or indirectly disclose the identity of the individuals mentioned in the reports.

9) Limited data retention periods

Data relating to a report found to be unsubstantiated by the entity in charge of processing such reports should be deleted immediately.

Data relating to reports that required verification should not be kept more than two months after the verification work is closed, unless disciplinary action is taken or court proceedings are filed against the individual incriminated or the author of an abusive report.

10) Accurate information provided to incriminated person

In accordance with articles 6 and 32 of the Data Protection Act, an identified individual that was incriminated by a report should be notified by the person in charge of the process as soon as data concerning him or her is recorded, whether electronically or not, so as to enable him or her to object promptly to his or her data being processed.

At any rate, the reported individual should not be informed before indispensable protective measures have been taken.

The information is given in a way which ensures that the reported person is properly notified.

Such information to the reported employee should include the identification of the entity in charge of handling the system, charges brought against him or her, what departments will receive the report as well as how to exercise his or her right of access and rectification.

11) Complying with rights of access and rectification

In accordance with articles 39 and 40 of the Data Protection Act, any person identified in the professional whistleblowing process may access his or her data and request the rectification or deletion thereof, if applicable.

His or her right of access does not entitle him or her to request the disclosure of information about third parties, such as the whistleblower's identity.
END TEXT.

¶6. (SBU) Post would appreciate any guidance on the draft.
STAPLETON